

SUMMARY

AT&T Wireless Services, Inc., ("AWS"), Lucent Technologies Inc., ("Lucent") and Ericsson Inc. ("Ericsson") bring this petition under Section 107(c) of the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. §§ 1001 et seq., seeking an extension of CALEA's October 25, 1998, compliance date to at least October 24, 2000, because CALEA-compliant hardware and software will not be available within the compliance period.

This extension request is urgent. Further development of a CALEA solution in the face of the unstable industry standard would expose the vendors to potentially enormous expense of money and engineering resources because any modification to the existing industry standard could require significant changes in Lucent's or Ericsson's individual CALEA solution. Given the current stage of development, both Lucent and Ericsson will soon reach a "point of no return" whereby development commitments toward the existing standard will become irreversible. Thus, AWS and its vendors require an immediate response to this extension request.

Accordingly, AWS, Lucent and Ericsson request that the Commission grant the extension as soon as possible, effective October 25, 1998, for the full 2-year period.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

In the Matter of _____)
)
)
Implementation of Section 103 of)
the Communications Assistance for)
Law Enforcement Act)
)
)
_____)

RECEIVED

MAR 27 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

JOINT MOTION TO DISMISS

CTIA'S JULY 16, 1997 PETITION FOR RULEMAKING

1. The Department of Justice and the Federal Bureau of Investigation (FBI), on behalf of themselves and other federal, state, and local law enforcement agencies, hereby move for an order dismissing the Cellular Telecommunications Industry Association's (CTIA's) July 16, 1997 Petition for Rulemaking.¹ This motion is made pursuant to Sections 1.2 and 1.401(e) of the Federal Communications Commission Rules on the grounds that CTIA's petition is now moot and plainly does not warrant the attention of the Commission. 47 C.F.R. §§ 1.2 and 1.401(e).

I. BACKGROUND

2. On July 16, 1997, CTIA filed a Petition for Rulemaking requesting that the Commission

¹ CTIA's petition has not yet been assigned a docket number.

establish an electronic surveillance technical standard to implement Section 103(a) of the Communications Assistance for Law Enforcement Act (CALEA).² 47 U.S.C. § 1002(a). The petition stated that no industry standard had been adopted at that time because of an impasse between the industry and law enforcement over the capabilities that should be incorporated into the standard. CTIA requested that the Commission adopt as the standard the then-current industry consensus document which it attached to the petition.

3. The substantive legal basis for CTIA's petition was Section 107(b) of CALEA, 47 U.S.C. § 1006(b). That provision states that if industry associations or standard-setting organizations "fail to issue" technical requirements or standards, then the Commission may be petitioned to establish those standards. As of the date of the petition -- July 16, 1997 -- CTIA was correct in alleging that there was a failure on the part of industry and standard-setting organizations to issue technical requirements or a standard, as none existed.

4. However, on December 8, 1997, the premise for CTIA's petition ceased to exist. On that date, members of the telecommunications industry approved interim standard J-STD-025, despite its failure to include the assistance capabilities that law enforcement had consistently maintained were required by Section 103(a) of CALEA, 47 U.S.C. § 1002(a). The standard was then published by the Telecommunications Industry Association (TIA) and the Alliance for Telecommunications

² The Communications Assistance for Law Enforcement Act, Pub L. No. 103-414, 108 Stat. 4270 (1994) (codified as amended in 18 U.S.C. and 47 U.S.C.).

II. DISCUSSION

CTIA'S PETITION IS MOOT AND DOES NOT WARRANT

CONSIDERATION BY THE COMMISSION.

5. CTIA's petition should be dismissed on the grounds that it is moot and does not warrant consideration by the Commission. Section 1.1401(e) of the Commission rules provides:

Petitions which are moot, premature, repetitive, frivolous, or which plainly do not warrant consideration by the Commission may be denied or dismissed without prejudice to the petitioner.

47 C.F.R. § 1.401(e).

A matter is moot when it presents no actual controversy or where the issues have ceased to exist.⁴

Here, CTIA's petition was premised on the fact that no industry standard had been adopted at the time of its filing. After CTIA filed its petition, industry did adopt a standard. It thereby rendered CTIA's petition moot.

6. For the same reasons that the petition is moot, CTIA's petition should also be dismissed on the grounds that "it does not warrant consideration by the Commission."⁵ In addition, CTIA's petition does not warrant consideration by the Commission in light of the Joint Petition for

³ See Attachment A.

⁴ BLACKS LAW DICTIONARY 1008 (6th Ed. 1990) (defining "moot case").

⁵ 47 C.F.R. § 1.401(e).

Expedited Rulemaking being filed separately by the Department of Justice and the FBI on behalf of law enforcement. The Joint Petition for Expedited Rulemaking alleges and demonstrates that the interim industry standard is "deficient" as that term is used in Section 107(b) of CALEA. In light of events that have taken place since the filing of CTIA's petition, the petition filed by the Department of Justice and the FBI supersedes CTIA's petition in terms of relevancy and accuracy. There is simply no reason to keep CTIA's outdated petition pending.

III. CONCLUSION

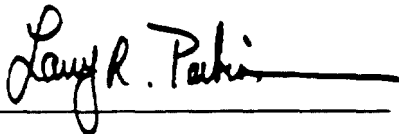
7. For the foregoing reasons, the Department of Justice and the FBI respectfully request that CTIA's July 16, 1997, Petition for Rulemaking be dismissed.

Date: March 27, 1998

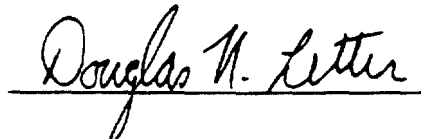
Respectfully submitted,

Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

Handwritten signature of Larry R. Parkinson in cursive script, underlined.

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Handwritten signature of Douglas N. Letter in cursive script, underlined.

Stephen W. Preston
Assistant Attorney General
Douglas N. Letter
Appellate Litigation Counsel
Civil Division, Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

Before the
Federal Communications Commission
Washington, D.C. 20554

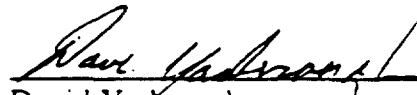
Certificate of Service

)
)
In the Matter of:)
)

Implementation of Section 103 of)
the Communications Assistance for Law)
Enforcement Act)
)
_____)

I, David Yarbrough, a Supervisory Special Agent in the office of the Federal Bureau of Investigation (FBI), 14800 Conference Center Drive, Suite 300, Chantilly, Virginia 20151, hereby certify that, on March 27, 1998, I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of the herewith Motion to Dismiss in the above-referenced proceeding, the original of which is filed herewith and upon the parties identified on the attached service list.

DATED at Chantilly, Virginia this 27th day of March, 1998.


David Yarbrough

**In the Matter of
Implementation of Section 103 of the
Communications Assistance for Law Enforcement Act**

Service List

***The Honorable William E. Kennard, Chairman**
Federal Communications Commission
1919 M Street, N.W.-Room 814
Washington, D.C. 20554

***The Honorable Harold Furchtgott-Roth, Commissioner**
Federal Communications Commission
1919 M Street, N.W.-Room 802
Washington, D.C. 20554

***The Honorable Susan Ness, Commissioner**
Federal Communications Commission
1919 M Street, N.W.-Room 832
Washington, D.C. 20554

***The Honorable Michael Powell, Commissioner**
Federal Communications Commission
1919 M Street, N.W.-Room 844
Washington, D.C. 20554

***The Honorable Gloria Tristani, Commissioner**
Federal Communications Commission
1919 M Street, N.W.-Room 826
Washington, D.C. 20554

***Christopher J. Wright**
General Counsel
Federal Communications Commission
1919 M Street, N.W.-Room 614
Washington, D.C. 20554

***Daniel Phythyon, Chief**
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W.-Room 5002
Washington, D.C. 20554

*David Wye
Technical Advisor
Federal Communications Commission
2025 M Street, N.W.-Room 5002
Washington, D.C. 20554

*A. Richard Metzger, Chief
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W.-Room 500B
Washington, D.C. 20554

*Geraldine Matise
Chief, Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 235
Washington, D.C. 20554

*Kent Nilsson
Deputy Division Chief
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 235
Washington, D.C. 20554

*David Ward
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 210N
Washington, D.C. 20554

*Marty Schwimmer
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 290B
Washington, D.C. 20554

*Lawrence Petak
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554

***Charles Iseman**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554 Policy Division

***Jim Burtle**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554

Matthew J. Flanigan
President
Telecommunications Industry Association
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834

Tom Barba
Stephoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795

Thomas Wheeler
President & CEO
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036

Albert Gidari
Perkins Coie
1201 Third Avenue
40th Floor
Seattle, Washington 98101

Jay Kitchen
President
Personal Communications Industry Association
500 Montgomery Street
Suite 700
Alexandria, VA 22314-1561

Roy Neel
President & CEO
United States Telephone Association
1401 H Street, N.W.
Suite 600
Washington, D.C. 20005-2164

*International Transcription Service, Inc.
1231 20th Street, N.W.
Washington, D.C. 20036

***HAND DELIVERED**

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED
MAR 27 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of:

Establishment of Technical Requirements
and Standards for Telecommunications
Carrier Assistance Capabilities Under the
Communications Assistance for Law
Enforcement Act

Docket No. _____

JOINT PETITION FOR EXPEDITED RULEMAKING

Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Stephen W. Preston
Deputy Assistant Attorney General

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

*DAVID L. YARRINGTON
SUPERVISOR, SPECIAL AGENT
FED. BUREAU OF INVESTIGATION
WASHINGTON DC*

No. of Copies rec'd
List ABCDE

CHG

TABLE OF CONTENTS

SUMMARY	1
I. INTRODUCTION	3
II. BACKGROUND	5
A. Pre-CALEA Electronic Surveillance	6
B. The Enactment of CALEA	11
C. Post-Enactment Developments	19
III. DISCUSSION	23
A. THE COMMISSION SHOULD ESTABLISH TECHNICAL REQUIREMENTS AND STANDARDS THAT MEET THE REQUIREMENTS OF CALEA	23
1. The Commission Has the Authority To Entertain this Petition And Grant the Relief Requested	23
2. Action by the Commission Is Needed To Correct the Deficiencies of the Interim Standard and Meet the Requirements of CALEA	24
a. Ability to intercept the communications of all parties in a conference call supported by the subscriber's service or facilities	27
b. Ability to access call-identifying information	33
c. Timely delivery of call-identifying information	49
d. Automated delivery of surveillance status information	52
e. Standardization of delivery interface protocols	57
3. The Technical Requirements and Standards of the Proposed Rule Satisfy the Criteria of Section 107(b) of CALEA	59
B. THE COMMISSION SHOULD CONSIDER THIS MATTER ON AN EXPEDITED BASIS	64
IV. CONCLUSION AND RELIEF REQUESTED	66

SUMMARY

The Communications Assistance for Law Enforcement Act (CALEA) was enacted in 1994 to ensure that ongoing technological changes in the telecommunications industry would not compromise the ability of federal, state, and local law enforcement agencies to engage in lawful surveillance activities. To that end, Section 103 of CALEA explicitly obligates telecommunications carriers to ensure that their equipment, facilities, and services are capable of expeditiously isolating and delivering to law enforcement agencies all communications and call-identifying information that law enforcement is authorized to acquire.

CALEA contemplates that the communications industry, acting in consultation with law enforcement agencies, will develop technical requirements and standards that implement the assistance capability requirements of Section 103 and act as a "safe harbor" for industry. At the same time, Congress recognized that the standards developed by industry might be inadequate to carry out the statutory mandates. Section 107(b) of CALEA therefore authorizes the Commission to issue rules establishing additional technical requirements and standards if a government agency believes that an industry standard is deficient.

The Department of Justice and the Federal Bureau of Investigation (FBI) are filing this petition to initiate an expedited rulemaking proceeding under Section 107(b) of CALEA and related provisions. They are taking this step because, after careful consideration and consultation, they have determined that the interim technical standard adopted by industry is seriously deficient. In the view

of the Department of Justice, the FBI, and other federal, state and local law enforcement agencies, the industry's interim standard is not adequate to ensure that law enforcement will receive all of the communications content and call-identifying information that carriers are obligated to deliver under Section 103 and the applicable electronic surveillance statutes. The interim standard also fails to ensure that information will be delivered in a timely manner. Unless the deficiencies in the interim standard are corrected by the Commission, information that is critical to public safety and law enforcement will be lost, and Congress' goal of preserving the surveillance capabilities of law enforcement agencies in the face of technological changes will be seriously compromised.

This petition explains why the industry's interim standard is deficient and what services and features should be added to correct its deficiencies and carry out the mandates of CALEA. The petition is accompanied by a proposed rule that sets forth, in specific terms, the changes that the petitioners believe should be adopted by the Commission. The petitioners request that the Commission initiate an expedited rulemaking proceeding leading to the adoption of the proposed rule and any other requirements and standards that the Commission determines to be appropriate under Section 107(b).

I. INTRODUCTION

1. The Department of Justice and the FBI, on behalf of themselves and other federal, state, and local law enforcement agencies,¹ respectfully request the Commission to initiate an expedited rulemaking to establish technical requirements or standards for electronic surveillance assistance by telecommunications carriers under the Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in 18 U.S.C. and 47 U.S.C.). This petition is filed pursuant to Sections 103 and 107(b) of CALEA (47 U.S.C. §§ 1002 and 1006(b)), Sections 4(i) and 229(a) of the Communications Act of 1934 (47 U.S.C. §§ 154(i) and 229(a)), and Section 1.401(a) of the Commission's rules (47 C.F.R. §1.401(a)).

2. Section 103 of CALEA (47 U.S.C. § 1002) imposes affirmative obligations on telecommunications carriers to ensure that their equipment, facilities, and services are capable of providing specified assistance to law enforcement in the conduct of authorized electronic surveillance. Under Section 107(a) of CALEA (47 U.S.C. § 1006(a)), a carrier is deemed to be in compliance with Section 103 if it is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization to meet the requirements of Section 103. However, compliance with the industry standard is merely one way

¹ Following passage of CALEA, the FBI assembled the Law Enforcement Technical Forum ("LETf"), consisting of 21 representatives from federal agencies and 30 from state and local law enforcement agencies, as well as the Royal Canadian Mounted Police. LETf members participated in the development of this petition. In turn, the FBI and the LETf have coordinated CALEA implementation issues, and developed consensus positions, with several hundred of the major law enforcement agencies and prosecutors' offices across the United States.

of assuring compliance with Section 103: a carrier can satisfy its obligations by any means that meet Section 103's underlying assistance capability requirements. Moreover, if a government agency believes that technical requirements or standards adopted by an industry association or standard-setting organization are deficient, it may petition the Commission under Section 107(b) (47 U.S.C. § 1006(b)) to establish, by rule, technical requirements or standards that meet the requirements of Section 103.

3. On December 8, 1997, the Telecommunications Industry Association (hereafter referred to as "TIA") published an interim technical standard ("interim standard") concerning electronic surveillance assistance requirements for telecommunication carriers providing wireline, cellular, and personal communications services. This petition is being filed because the interim standard lacks specified electronic surveillance assistance capabilities and related provisions that are required by CALEA. The Department of Justice and the FBI ask the Commission, by rule, to supplement the interim standard by incorporating additional capabilities and provisions that will satisfy the requirements of Sections 103 and 107(b) of CALEA. A proposed rule that sets forth requested technical requirements and standards is contained in Appendix 1 of this petition.

4. The technical requirements and standards sought in this petition are intended to operate in addition to, not in lieu of, the interim standard. Thus, the interim standard should not be stayed pending a determination of this rulemaking.

5. The Department of Justice and the FBI urge the Commission to consider this matter on an expedited basis so that the deficiencies of the interim standard can be corrected as soon as possible. Expedited consideration will further the strong public safety interest in preserving law enforcement's ability to conduct effective, lawfully authorized electronic surveillance in its continuing efforts to combat criminal activity. Expedited consideration also will help to avoid delay in the development, manufacture, and deployment of CALEA-compliant solutions for existing and future equipment so that law enforcement agencies can effectively fulfill their public functions.

II. BACKGROUND

6. This petition concerns statutory obligations placed on telecommunication carriers by CALEA. To understand fully the nature and scope of those obligations, it is essential to understand the background of this legislation. As described below, CALEA was passed primarily at the behest of the FBI and other law enforcement agencies, despite opposition from the telecommunications industry, in order to ensure that lawful electronic surveillance as an invaluable crime-fighting tool is not thwarted by technological and structural changes in the telecommunications industry. CALEA is designed to preserve the ability of federal, state, and local law enforcement agencies to carry out lawful surveillance in the face of these changes.

A. Pre-CALEA Electronic Surveillance

7. For many decades, law enforcement agencies have been able to employ court-ordered electronic surveillance successfully in collecting evidence in criminal investigations. The principal statutory authority allowing these agencies to conduct electronic surveillance is contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter "Title III"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA") (codified at 18 U.S.C. §§ 2510 et seq.). In 1986, Congress modified Title III in order to update its provisions and clarify federal privacy protections and electronic surveillance standards in light of changes in computer and telecommunications technologies. In addition, Congress added a court order requirement for "pen registers" and "trap and trace" devices. (18 U.S.C. §§ 3121 et seq.).² ("Pen registers" do not intercept the contents of calls, but instead record outgoing dialed digits, tones, and any other signals from a subscriber's telecommunications equipment or facilities; "trap and trace" devices provide information concerning the origination of incoming calls.)

8. Title III imposes significant responsibilities on law enforcement officers in order to protect privacy to the maximum extent possible while allowing evidence gathering through electronic surveillance. For example, a law enforcement agency is obligated to demonstrate that other practical investigative techniques are unavailing before seeking electronic surveillance authorization (18

² The history of federal wiretap legislation is described in the Commission's Notice of Proposed Rulemaking in In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, FCC 97-356 (released Oct. 10, 1997), at 4-8 (cited hereafter as "FCC Notice").

U.S.C. § 2518(3)(c)), and it must minimize interception of non-criminal conversations (18 U.S.C. § 2518(5)). In addition, tapes of intercepted communications must be sealed at the end of the interception period (18 U.S.C. § 2518(8)), and only authorized disclosures of such material are permitted (18 U.S.C. §§ 2511(1)(c) and 2517).

9. Law enforcement agencies have often conducted electronic surveillance with the assistance of the telecommunications industry, but sometimes have been forced to proceed without the industry's cooperation. In some instances, certain service providers have refused to render needed assistance to law enforcement officers even when surveillance was judicially authorized. See, e.g., Application of United States, 427 F.2d 639 (9th Cir. 1970). In light of this problem, in 1970, Congress amended Title III to make clear the responsibility of telephone service providers to provide assistance to law enforcement personnel. Specifically, Congress amended Title III to provide that interception orders shall "direct that a provider of wire or electronic communication service * * * shall furnish the applicant [for the order] forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider * * * is according the person whose communications are to be intercepted." 18 U.S.C. § 2518(4).

10. Despite the 1970 amendments to Title III, telephone service providers have continued in certain instances to refuse full cooperation for criminal investigations, forcing law enforcement officials to seek compulsion from the courts. See, e.g., United States v. New York Telephone Co., 434 U.S. 159 (1977) (compelling telephone company to provide assistance to the FBI in installing

pen registers); United States v. Mountain States Telephone and Telegraph Co., 616 F.2d 1122 (9th Cir. 1980) (compelling telephone company to program computerized electronic switching equipment so that the IRS could determine numbers from which incoming calls to target were being made); Michigan Bell Telephone Co. v. United States, 565 F.2d 385 (6th Cir. 1977) (compelling telephone company to employ both manual and electronic tracing devices on specified telephones).

11. Prior to 1984, the great majority of local and long distance telecommunications were carried by AT&T, which held a virtual monopoly on these services. This dominance resulted in a largely homogeneous telephone network in which the technology of the equipment used to conduct business was generally uniform throughout the network. The telephone system was largely based on "analog" technology, which converted voices into electronic patterns that mimic natural sound waves. The electronic impulses would then travel over copper wires, and were directed to the receiver by electronic contact switches. Law enforcement agents were consistently able to conduct electronic surveillance by gaining access to telephone lines between the service provider's central office and a telephone subscriber's home or office (the "local wire loop"). These interceptions were highly effective for the existing technologies, and law enforcement agents were able to intercept the content of all communications supported by a subscriber's service or carried over the subscriber's facilities, as well as information concerning the nature of any calls (such as from which numbers they came and to which numbers they went). In addition, these agents could verify the accuracy, integrity, and operability of the surveillance throughout the interception period.

12. Thus, until fairly recently, law enforcement officers could obtain all information available to the telephone service provider concerning use of the services that it rendered to a particular subscriber, including when and to which numbers calls were made, when and from which numbers calls were received, and the complete contents of those calls. In other words, everything then technologically possible to know about the telephone service being provided was available to authorized law enforcement officers. Further, there were no technological limitations on the number of interceptions that could be conducted.

13. This situation changed considerably and rapidly in the past 20 years, particularly following the breakup of AT&T in 1984. The number of long distance and local service providers has increased dramatically, and this number has expanded even further with the advent of wireless technologies. Law enforcement agencies must now deal with well over one thousand different telecommunications service providers who are employing a host of new technological developments. These developments are possible in part because analog technology is being replaced by digital technology, under which a communication is converted by computer into streams of binary data representing the digits "0" and "1". Rather than being routed by an electrical contact switch, a call is typically routed by a computer at the carrier's switching facility.

14. As this petition indicates, the development of new telecommunications technologies has provided subscribers with a range of new services that enable them to accomplish tasks with their telephone systems that could not be done before. For example, in the past decade or so, the following services became widely available to subscribers: call forwarding; call transferring; direct

implementation by a subscriber of new services: voice-activated dialing and speed dialing from the service provider's centralized facility; the ability to have voice "mail box" message systems accessed by a subscriber; and the ability to initiate a multi-party call and then depart, leaving the other parties still connected.

15. These new telecommunications technologies allow for the efficient transmission of multiple, simultaneous communications of various subscribers over fiber optic lines and wire facilities. Features such as call forwarding permit customers to redirect calls, thereby no longer requiring that communications be transmitted to the same specific location or through the same wire line loop. Likewise, "follow me" features expand the nature of call forwarding to national dimensions. And personal communications services enable users to define their own set of subscribed services, use any fixed or mobile terminal or telephone instrument, and make and receive calls across multiple networks without regard to their location. All of these services have removed a telephone subscriber from a fixed local wire loop that could be tapped by law enforcement agents, and thereby have greatly hampered the ability to conduct court approved electronic surveillance. See also FCC Notice at 10 ("In addition to the proliferation of services currently offered, the increase in the sheer number of service providers further complicates efforts to conduct the authorized implementation of electronic surveillance").

16. Moreover, as new technology is deployed, the principal technique used for electronic surveillance of telecommunications will also change. In the past, law enforcement officers typically utilized their own equipment physically to tap into an existing wire leading to a subscriber's house

or business. However, with the advent of digital transmissions and the use of a telecommunications carrier's computer to provide services at a centralized point, electronic surveillance will often be accomplished through the use of software employed by the carrier to route authorized information to law enforcement officers.

B. The Enactment of CALEA

17. In March 1994, FBI Director Freeh informed Congress that the telecommunications technological revolution was having a devastating impact on the ability of law enforcement officers to carry out their essential electronic surveillance duties. See Joint Hearings on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House of Representatives Comm. on the Judiciary, 103d Cong., 2d Sess. 5-6, 14 (March 18, 1994) (statement of Louis J. Freeh). Director Freeh explained to Congress that "[i]ndustry representatives have bluntly told law enforcement that the existing telecommunications systems and networks will thwart court authorized intercepts" (*id.* at 24). The developments in telecommunications technology "often prevent, and will continue to prevent common carriers from providing law enforcement with access to all of the communications and dialing information that are the subject of electronic surveillance and pen register court orders" (*id.* at 24). The telecommunications industry had been telling the FBI that "there is a serious problem, and they have been forecasting that within a very short period of time they will not be able to service